SOC Analyst Interview Prep — Rahul C

Questions are grouped by category, pulled directly from what's on your resume, with suggested answers you can personalize. Swap in real numbers/details where I've used placeholders like [X].

---

1. Resume Walkthrough / Background

Q: Walk me through your resume / Tell me about yourself. A: "I have about 4 years of combined experience across IT Support and Security Operations. I started at Infosys BPM handling IT support — resolving hardware, software, and network issues, managing Active Directory accounts, and doing patch management and vulnerability checks. That gave me a strong foundation in enterprise IT systems. Since January 2025, I've been working as a SOC Analyst at Moder Solution India, where I monitor and triage 100+ security alerts daily using Splunk in a 24x7 SOC. I investigate phishing, suspicious logins, and endpoint malware using tools like VirusTotal, ANY.RUN, and Wireshark, apply the MITRE ATT&CK framework for analysis, and maintain 98% SLA compliance. I'm looking to grow further into deeper threat hunting and detection engineering work."

Q: Why did you move from IT Support to SOC/Security? A: "IT Support gave me hands-on exposure to endpoint compliance, patch management, and vulnerability checks, and I found the security side of those tasks the most interesting part of the job. I started pursuing SOC-specific certifications — like SOC Incident Handling & Response and SIEM Log Analysis — and transitioned into a dedicated SOC Analyst role where I could focus fully on monitoring, detection, and incident response."

Q: Why are you looking to leave your current role / applying here? A: Personalize this — focus on growth (L2 responsibilities, exposure to more advanced tooling, threat hunting) rather than anything negative about your current employer.

---

2. Core Technical Questions (SIEM / Splunk)

Q: Walk me through how you triage an alert in Splunk. A: "First, I look at the alert context — source, destination, user, and the rule that triggered it. I check for false-positive indicators based on the runbook. If it looks legitimate, I pull related logs (auth logs, proxy logs, endpoint logs) to build a timeline. For example, on a suspicious login alert, I'd check geolocation, login history, MFA status, and whether the account showed any other anomalous activity. I correlate this with threat intel — checking IPs/hashes in VirusTotal or IPVoid — before deciding to escalate, contain, or close as benign, all within our SLA window."

Q: What's the difference between a false positive and a true positive, and how do you reduce false positives? A: "A false positive is an alert that looks malicious but has a

legitimate explanation — e.g., a login flagged for a new location that turns out to be an employee traveling. I reduce false positives by tuning correlation rules where I have visibility, documenting recurring benign patterns in the runbook, and using enrichment (asset ownership, known VPN ranges, business context) before escalating, so SOC time is spent on genuine threats."

Q: What SIEM correlation rules or use cases have you worked with? A: Describe 2-3 concrete examples from your actual experience: e.g., failed login threshold alerts, malware detection via endpoint agent, phishing email alerts, impossible travel/geo-velocity alerts. Be specific about what data sources fed the rule.

Q: How do you investigate a phishing alert end-to-end? A: "I start with the email headers to check SPF/DKIM/DMARC results and sender authenticity. I check the URL/attachment reputation using VirusTotal and ANY.RUN — ANY.RUN in particular helps me detonate suspicious attachments/links in a sandbox to observe behavior. I check MXToolbox for domain reputation. If it's confirmed malicious, I check whether other users received the same email, block the sender/domain/hash, and coordinate with IT to remove the email from inboxes and reset credentials if anyone clicked."

Q: What's your process for investigating an endpoint malware alert? A: "I check the EDR/AV alert details — file hash, process tree, and what triggered detection. I run the hash through VirusTotal for reputation, isolate the endpoint if needed, and check Code42 or asset logs for any data exfiltration risk. I document the timeline, coordinate with the endpoint/IT team for remediation, and update the incident ticket with root cause and resolution steps."

---

3. MITRE ATT&CK

Q: How do you use the MITRE ATT&CK framework in your daily work? A: "I use it to map alerts to specific tactics and techniques — for example, classifying a suspicious PowerShell execution under Execution (T1059) or a phishing email under Initial Access (T1566). This helps standardize how we describe incidents in reports and helps identify patterns, like if we're seeing repeated attempts under the same technique from different sources, which could indicate a coordinated campaign."

Q: Can you give an example of mapping a real incident to ATT&CK? A: Prepare one real example from your SOC work — walk through: alert → technique/tactic identified → why you classified it that way → outcome.

---

4. Tools-Specific Questions

Q: What's the difference between Wireshark and Splunk, and when would you use each? A: "Splunk is my primary SIEM for aggregated log monitoring, correlation, and alerting across the environment. Wireshark I use for deep packet-level analysis — when I need to

inspect actual network traffic, like confirming data exfiltration or unusual protocol behavior that logs alone don't show clearly."

Q: How do you use Nessus in your workflow? A: "Nessus is for vulnerability scanning — I use it to run scheduled scans, review CVSS-scored findings, and prioritize remediation with the infrastructure team based on severity and exploitability, particularly for internet-facing or critical assets."

Q: What's the role of a WAF and Proxy in your security stack? A: "The WAF protects web applications from attacks like SQLi and XSS at the application layer, while the proxy (and Zscaler in our case) enforces web filtering, inspects outbound traffic, and helps detect C2 communication or access to malicious domains. Together with IDS/IPS and firewall logs, they give layered visibility that I correlate in Splunk."

---

5. Scenario / Judgment Questions

Q: You get 50 alerts in your queue and 10 minutes left in your shift. How do you prioritize? A: "I triage by severity and business impact first — critical assets, confirmed malware, or anything indicating active compromise takes priority over routine alerts. I'd handle or at least stabilize the highest-severity items, then write a clear, detailed shift handover for anything unresolved so the incoming analyst has full context and nothing falls through the cracks."

Q: You suspect an alert is a true positive but you're not 100% sure. What do you do? A: "I escalate per the runbook rather than sitting on it. It's better to escalate a potential false positive than to miss a real incident. I'd document my findings, reasoning, and evidence gathered so far, and hand it to L2/IR with full context."

Q: How do you handle a disagreement with a senior analyst or SME about how to handle an incident? A: "I'd present my findings and reasoning clearly, back it with evidence from the logs, and stay open to their perspective since they may have context I don't. If we still disagree, I'd follow escalation procedure and let the incident lead make the final call, since consistency in IR process matters more than being 'right' in the moment."

Q: Tell me about a time you caught something others might have missed / a challenging incident you handled. A: Prepare a real STAR-format story (Situation, Task, Action, Result) from your Moder Solution or Infosys experience — even a smaller incident works well if you can show your reasoning process clearly.

---

6. Behavioral Questions

Q: How do you stay updated on new threats and vulnerabilities? A: "I follow threat intel feeds, CVE advisories, and vendor security bulletins relevant to our tech stack. I also review MITRE ATT&CK updates and take note of new certifications/training to keep my SIEM and threat-hunting skills current — like the Splunk Fundamentals training I completed."

Q: How do you handle working in a 24x7 shift-based environment? A: "I stay organized with clear documentation and shift handovers so continuity isn't lost between shifts. I've maintained 98% SLA compliance by prioritizing effectively and following runbooks consistently, even under alert volume pressure."

Q: Where do you see yourself in 2-3 years? A: "I want to grow from L1 into L2/L3 SOC responsibilities — taking on more threat hunting, incident response leadership, and eventually specializing further, possibly in detection engineering or threat intelligence."

---

7. Questions You Should Ask Them

- What SIEM and tools does the team primarily use, and would I be working with a similar stack to Splunk/Wireshark/VirusTotal?
- What does the escalation path look like from L1 to L2/L3 here?
- How is the SOC team structured — in-house, hybrid with an MSSP, or fully outsourced?
- What's the typical alert volume per shift, and how mature are your detection rules/playbooks?
- What growth path exists for L1 analysts on this team?

Quick Tips

- Have 2-3 real, specific incident stories ready in STAR format — interviewers weight concrete examples far more than general process descriptions.
- Know the "why" behind every tool on your resume, not just what it does — be ready for "when would you NOT use X."
- Be honest about the boundary of your hands-on experience (e.g., if you've only observed rule-tuning vs. done it yourself) — SOC interviewers often probe depth quickly.